Vertragsgestaltung rund um Big Data

Weber, Rolf H ; Staiger, Dominic N

ROLF H. WEBER*/DOMINIC N. STAIGER**

Vertragsgestaltung rund um Big Data

Inhaltsverzeichnis

I. Einleitung

Das Ziel von Big Data liegt in der Sammlung und Auswertung umfassender Datenbestände verschiedenster Herkunft in Hochleistungsdatenbanken. Für die detaillierten Datenanalysen ist die Art der Daten (z.B. Text, Bild, Video) ebenso irrelevant wie die Qualität der Daten (z.B. strukturierte oder unstrukturierte Daten). Die Herkunft der Daten spielt auch keine Rolle; die Sammlung der Daten kann auf unternehmensinternen Quellen, auf durch Drittpersonen zur Verfügung gestellten Quellen oder auf frei zugänglichen Quellen beruhen. Meist werden die Daten jedoch vom Nutzer eines Dienstes selbst zur Verfügung gestellt.[1]

* Prof. Dr., Ordinarius, Privat-, Wirtschafts- und Europarecht, Zentrum für Informations- und Kommunikationsrecht ZIK, Universität Zürich.

** Assistent, Lehrstuhl Weber, Privat-, Wirtschafts- und Europarecht Universität Zürich.

1 Vgl. ROLF H. WEBER, Big Data: Sprengkörper Des Datenschutzrechts?, Weblaw Jusletter IT, 11. Dezember 2013, Rz. 3–7.

Für die Problematik der vertraglich vereinbarten «Organisation» von Big Data stellt sich die besondere Herausforderung, dass die Sammlung der Daten an sich unsichtbar sowie die Instrumente und Techniken kaum nachvollziehbar sind, insbesondere im Lichte der physischen, technischen und rechtlichen «Layers», auf denen Daten gesammelt werden. Aus diesem Grunde ist die Frage zu stellen, inwieweit Überwachungsfunktionen in einem komplexen Big-Data-Analytics-System nicht offen zu legen und einer vertraglichen Regelung zuführbar zu machen sind;[2] dies gilt insbesondere für die geographischen Metadaten, welche zentral für die Big Data Analytics sind.[3]

Diese Transparenzschaffung erleichtert insbesondere die Verwirklichung des Rechts einer Person festzulegen, wer wie mit den Daten umgehen darf, und zwar als Ausdruck der Souveränität über die eigenen persönlichen Daten. Durch die Schaffung von Transparenz und vertragliche Beeinflussungsmöglichkeiten lässt sich gegebenenfalls ein gesundes Gleichgewicht zwischen der «Macht» derjenigen, welche die Daten generieren, und der Stellung derjenigen, die durch Indifferenzen und entsprechende Bearbeitungsentscheide betroffen sein können, herbeiführen.[4]

Insbesondere hat der Big-Data-Nutzer diejenigen Personen, über welche Daten gesammelt werden, darüber zu informieren, inwiefern durch zukünftige Analysemethoden ihre Daten genutzt werden sollen. Den betroffenen Personen muss es dabei erlaubt sein, einer Nutzung, mit welcher sie nicht einverstanden sind, zu widersprechen. Aufgrund des damit verbundenen Aufwands sind jedoch einfache Systeme zu schaffen, um die Verwaltung dieser Berechtigungen übersichtlich und effizient zu gestalten.

Die Realität ist, aufgrund der oftmals leichtfertigen Datenherausgabe der Internetnutzer und der expansiven Nutzung ihrer Daten heute jedoch eine andere. Sehr grosse Datenbestände in Verbindung mit intelligenten Algorithmen und Cloud Technologien erlauben den Unternehmen, komplexe Berechnungen auszuführen und unterschiedlichste Hypothesen zum Kundenverhalten zu entwickeln und zu testen. Diese Vorhersagen basieren auf Aufzeichnungen des menschlichen Handelns und stellen damit eine für die Unternehmen zuverlässige Grundlage zur Einschätzung zukünftigen Wirtschaftsverhaltens dar.

---

2 BRUNO BAERISWYL, «Big Data» ohne Datenschutz-Leitplanken, digma 2013, 17.

3 RUDI KLAUSNITZER, Das Ende des Zufalls, Salzburg 2013, 133.

4 NEIL M. RICHARDS/JONATHAN H. KING, Three Paradoxes of Big Data, Stanford Law Review Online 66 (2013), 44, (http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big- data).

Diese Tatsache steht im Spannungsverhältnis zu den Datenschutzprinzipien, insbesondere dem Prinzip der Datenminimierung[5], sowie der freien Entscheidung des Einzelnen über die Verwendung seiner Daten. Die nachfolgenden Ausführungen untersuchen, inwieweit sich durch vertragliche Regelungen die Rahmenbedingungen von Big-Data-Analysemethoden privatautonom festlegen lassen. Dabei sind einerseits die Rahmenbedingungen für die Inanspruchnahme gesetzlich gegebener Rechte, und andererseits das Verständnis der Bürger für den Datenschutz zu verbessern.[6] Oftmals werden nämlich persönliche Daten freiwillig sozialen Netzwerken oder anderen Anbietern übergeben, welche diese Daten nur allzu gerne für ihre eigenen wirtschaftlichen Zwecke verwenden.[7]

II. Vertragliche Grundprinzipien

1. Konzeptionelle Ausgestaltung

Abgesehen von Datensammlungen, die ausserhalb jeglicher vertraglicher Beziehungen stattfinden und die im Falle der Verletzung datenschutzrechtlicher Prinzipien «nur» zu ausservertraglichen Ansprüchen des Betroffenen führen, sind insbesondere zwei vertragliche Konstellationen denkbar:

- Zwischen einem Unternehmen und einer Individualperson besteht eine vertraglich begründete Geschäftsbeziehung, die (auch) den Austausch von Daten nach sich zieht. Das Unternehmen verwendet die entsprechenden Daten für Big-Data-Analysen.
- Eine Individualperson beauftragt ein Unternehmen, vertraglich umschriebene, verarbeitungsspezifische Aufgaben im Rahmen von Datenbearbeitungen, Datensammlungen und Datenarchivierungen vorzunehmen.

Denkbar ist weiter ein Vertragsverhältnis, in welchem sich die eine Partei verpflichtet, im Interesse und im Auftrag der anderen Partei umfassend oder themenbezogen Big-Data-Analysen mit Blick auf eine Drittperson durchzuführen. In einem solchen Dienstleistungsvertrag fehlen Interessengegensätze zwischen den Vertragspartnern mit Blick auf die Einhaltung von Datenschutzgrundsätzen bei der Analysetätigkeit, weshalb diese Konstellation nicht weiter vertieft wird.

---

5 Das Bundesgericht spricht von objektiv tatsächlich benötigten Daten (BGE 125 II 473, E. 4).

6 Ira S. Rubinstein, Big Data: The end of privacy or a new beginning?, International Data Privacy Law 2013, Vol. 3, No. 2, 74.

7 Omer Tene, Privacy: The New Generation, International Data Privacy Law 2011, Vol. 1, No. 1, 15, 22–25.

2. Allgemeine Vertragsregeln

Für den Vertragsabschluss gelten die allgemeinen Regeln; ein Vertrag kommt bei Vorliegen übereinstimmender Willensäusserungen zustande. Schriftlichkeit ist an sich für die Gültigkeit des Vertrages nicht vorgesehen,[8] für die vorliegend interessierenden Geschäftstypen aber üblich. Mangels Vorliegens spezifischer gesetzlicher Vorgaben in der Vertragsgestaltung sind die Vertragspartner weitgehend frei, das konkrete Leistungsprogramm festzulegen. Die traditionellen Regeln des Schuldrechts gelten auch für den Fall, dass die Vertragsbeziehung durch einen elektronischen Austausch von Willenserklärungen zustande gekommen ist.

3. AGB als Vertragsbestandteil

Oft sind in der Praxis Datenschutzregeln entweder als elektronisch verfügbare gesonderte «Richtlinien» oder als Bestandteil von Allgemeinen Geschäftsbedingungen (AGB) ausgestaltet. Um die Rechtsgültigkeit von Online-AGB als Vertragsbestandteil zu gewährleisten, ist deren Existenz auf dem Bildschirm klar hervorzuheben. Der Kunde muss technisch auch in der Lage sein, die Online-AGB problemlos herunterzuladen und auf der eigenen Anlage zu kopieren.

Die Information über die Online-AGB ist so zu gestalten, dass der Kunde sie vor Abgabe seiner Willenserklärung (d.h. vor Anklicken des Bestell-Icons) wahrnimmt; konkret muss sich also der Hinweis auf die Online-AGB in räumlicher und zeitlicher Nähe des für den Bestellvorgang vorgesehenen Orts befinden. Die Grundsätze zur Kenntnisnahme von Online-AGB in zumutbarer Weise umfassen folgende Elemente:

- Gute Lesbarkeit (kein Kleindruck oder Platzieren der Bedingungen an schlecht sichtbarer Stelle);
- Übersichtlichkeit (Hervorheben der wichtigen Bestimmungen);
- Gut sichtbare Darstellung;
- Vertretbarer Umfang (keine übermässige Länge).[9]

Kommt es zu einem elektronischen Vertragsabschluss, sind die eben genannten strengen Regeln der AGB-Gültigkeitskontrolle einzuhalten. Eine Einwilligung zur Datenverarbeitung im Rahmen einer Big-Data-Analyse hat dabei infor-

---

[8] Es sei denn, die Parteien vereinbaren eine gewillkürte Form gemäss Art.16 OR.

[9] ROLF H. WEBER/CHRISTOPH A. WOLF, Fragmentarische E-Commerce Gesetzgebung, Weblaw Jusletter 18. Juni 2012, Rz. 5.

miert, ausdrücklich und spezifisch zu erfolgen.[10] Des Weiteren muss eine klare und transparente Vereinbarung von Verfügbarkeitswerten getroffen werden die als reine Leistungsbeschreibung und nicht als Leistungsbegrenzung ausgestaltet ist.[11]

Praktisch besteht bei Online-AGB das Problem, dass der akzeptierende Vertragspartner sich nur schwer einen Gesamtüberblick zu verschaffen vermag, weil das Blättern wie bei Papierseiten ausgeschlossen ist und sich durch die Scroll-Funktion bzw. die Volltextsuche nicht ohne weiteres kompensieren lässt. Aus diesem Grunde ist zu fordern, dass der Kunde ohne Schwierigkeiten auf die einzelnen Bestimmungen im Text zugreifen und sie vergleichen kann. Überdies ist bedeutungsvoll, insbesondere für spätere Beweiszwecke, dass die Möglichkeit besteht, die Online-AGB schnell und problemlos auszudrucken.

In Rahmen der AGB-Kontrolle wäre eine einheitliche Regelung zu begrüssen, welche es den Kunden der angebotenen Dienstleistung erlaubt, den Umfang der eingeräumten Datennutzung auf den ersten Blick festzustellen, weil sich eine ausdrückliche Einwilligung nur annehmen lässt, wenn der Kunde in der Lage ist, die Folgen der Datenbearbeitung abzuschätzen.[12] Wenn man davon ausgeht, dass Kunden heute bei der Einwilligung kaum je zu einer angemessenen Folgenabschätzung der Datenbearbeitung in der Lage sind, wird offensichtlich, dass die Datenschutzgesetzgebung den derzeitigen Realitäten nicht entspricht. Als Lösungsansatz denkbar wäre ein einheitliches Farbsystem, welches z.B. die Farben einer Ampel enthält. Intuitiv könnte damit der potenzielle Kunde feststellen, wie umfangreich das eingeräumte Nutzungsrecht und die Datenherausgabe in den jeweils vorliegenden AGB sind, ohne diese vollständig lesen zu müssen. Ob eine AGB-Einwilligung rechtsgenüglich den Kriterien der Voraussehbarkeit der möglichen Verwendung von Daten entspricht, ist durch die Rechtsprechung noch nicht geklärt; in der Lehre werden zum Teil Zweifel angebracht.[13]

Zum Thema der «Click-Wrap-Agreements» existiert umfangreiche Fachliteratur.[14] Jedoch ist die Rechtsprechung auf internationaler Ebene hierzu nicht ein-

---

10 THOMAS PROBST, Die richterliche Inhaltskontrolle Allgemeiner Geschäftsbedingungen im schweizerischen Recht: Ein rückblickender Ausblick in die Zukunft, in: PETER JUNG (ed), Europäisches Privatrecht in Vielfalt geeint (225–226).

11 BGH, Urteil vom 12.12. 2000 – XI ZR 138/00 (Köln); PETER BRÄUTIGAM, Vertragsgestaltung, in: PETER BRÄUTIGAM (Hrsg.), IT Outsourcing und Cloud Computing, Erich Schmidt Verlag, Berlin 2013, Rz. 200.

12 BAERISWYL (Fn. 2), 16.

13 BRUNO BAERISWYL, «Soziale Netzwerke» – Taktgeber für die Reform des Datenschutzrechts, in: WEBER/THOUVENIN (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012, 93, 100 f; ROLF H. WEBER, E-Commerce und Recht, 2. Aufl. Zürich 2010, 456 ff.

14 Vgl. JAY J. FORDER, Clickwrap agreements, signed documents and the objective test for contract formation. In S. KIERKEGAARD & P. KIEKEGAARD (ed.) Law across Nations: Gover-

heitlich. Als Grundsatz lässt sich aber festhalten, dass diese Form des Vertragsabschlusses den Grundprinzipien des Vertragsrechts folgen muss, d.h. es dürfen darin keine sehr unüblichen und extrem einseitig begünstigenden Bedingungen enthalten sein. Im Gegensatz zu «Browse-Wrap-Agreements» entfalten sie ihre bindende Wirkung mit dem Anklicken des «I accept» Knopfes. «Browse-Wrap-Agreements» hingegen versuchen die Wirkung der AGB auf den Nutzer der Website zu erstrecken, obwohl dieser nicht ausdrücklich, d.h. lediglich durch Nutzung der Website, solchen AGB zugestimmt hat. Die amerikanischen Gerichte haben in dieser Hinsicht entschieden, dass der Anbieter nachweisen muss, dass der Nutzer Kenntnis von den Bedingungen hatte, bevor er die Website nutzte.[15]

Für Unternehmen, welche ihren Big-Data-Bestand für eigene Zwecke gewinnbringend einsetzen möchten, kommt somit nur das Einholen der Zustimmung der Nutzer durch ein «Click-Wrap-Agreement» in Frage, welches ausdrücklich auf die in den AGB enthaltenen Datennutzungsrechte zu verweisen hat, um den Inhaltsvorschriften zu genügen. Hierbei setzt Art. 8 UWG der möglichen Datennutzung Grenzen, sofern diese ein Treu und Glauben verletzendes erhebliches Missverhältnis der vertraglichen Rechten und Pflichten herbeiführt.

III. Inhalt von Vertragsgestaltungskonzepten

1. Spezifische Elemente der Datensicherheit

Die Erfahrungen der letzten Jahre haben gezeigt, dass aus Sicht des Kunden die vertraglichen Gewährleistungen mit Bezug auf die Datensicherheit von besonderer Bedeutung sind. Dieses Anliegen gilt insbesondere, wenn die Daten und Dienstleistungen, die Gegenstand des Vertrages sind, einen hohen Grad an Sensitivität und Kritikalität aufweisen. Erschwerend kommt dazu, dass neu entwickelte Datenaufbewahrungskonzepte wie die Cloud zusätzliche Risiken verursachen.[16] Mögliche vertragliche Regelungspunkte sind:

- Vorgaben mit Blick auf die Datenlokalisation, nicht zuletzt auch angesichts der Schaffung sinnvoller Zugangsmöglichkeiten für den Kunden zu den Daten;

---

nance, policy & statutes (342–352); NANCY S. KIM, Wrap Contracts: Foundations and Ramifications, Oxford 2013.

15 Kwan v. Clearwire Corp., No. C09-1392JLR, 2012 WL 32380 (W.D. Wash. Jan. 3, 2012).

16 ROLF H. WEBER/DOMINIC N. STAIGER, Legal Challenges of Trans-border Data Flow in the Cloud, Weblaw Jusletter IT 15. Mai 2013 Rz. 27 ff.

- Regelung des grenzüberschreitenden Datenverkehrs, vor allem mit Ländern, die kein gleich hohes Datenschutzniveau aufweisen wie das Ursprungsland;
- Art und Weise der Aufbewahrung von Daten sowie Vorgaben mit Bezug auf die Vernichtung von Daten;
- Schaffung ausreichender Transparenz mit Bezug auf die Datenbearbeitung und Einrichtung sachgerechter Kontrollmöglichkeiten;
- Zulässigkeit des Einsatzes von weiteren Dienstleistungserbringern.

Konkrete Regelungsvorschläge sollten ebenfalls die automatisierte Meldung der ausgeführten Big-Data-Berechnungen, das Erfüllen adäquater Verschlüsselungsstandards und konkrete Rahmenbedingungen der Datenverwertung beinhalten.

In der Praxis ergeben sich jedoch bereits erste Schwierigkeiten in der Auslegung und Anwendung von Vertragsklauseln im Kontext des Datenschutzrechts. So statuiert z.B. Art. 13 des Datenschutzgesetzes, dass die Verarbeitung personenbezogener Daten zwar mit entsprechender Einwilligung der betroffenen Person vorgenommen werden darf, sich diese jedoch auf den ursprünglichen Zweck beziehen muss und somit bei späterer anderweitiger Verwendung erneut einer Zustimmung bedarf. Aufgrund der Datenmengen, welche gerade einen zentralen Kern der Big-Data-Datenverarbeitung darstellen, ist eine erneute Einwilligung jedes Einzelnen logistisch (auch aufgrund der zum Teil erfolgten Pseudonymisierung) kaum möglich.

Eine Pseudonymisierung führt zwar zu einem Verlust des Personenbezugs, welcher für die Anwendung des Datenschutzgesetzes notwendig ist, jedoch lässt sich dieser durch die eigentliche Big-Data-Technologie wieder herstellen.[17] Hierzu reichen drei charakteristische Merkmale einer Person aus.[18] Eine vertragliche Einwilligung der betroffenen Person zu jedweder zukünftigen Verarbeitung seiner personenbezogenen Daten ist ebenfalls AGB- und datenschutzrechtlich ausgeschlossen und stellt somit eine Grenze des vertraglich Möglichen dar.[19]

In der Schweiz findet auf Big Data Analytics insbesondere Art. 4 DSG Anwendung, welcher die Grundsätze der Datenverarbeitung und die Nutzung von personenbezogenen Daten statuiert. Es muss dabei der Zweck der Bearbeitung der Daten für den Nutzer klar erkennbar sein. Weiterhin dürfen Personendaten nur zu

---

[17] Baeriswyl, (n 2), 15; Melissa Gymrek/Amy L. Mcguire/David Golan/Eran Halperin/Yaniv Erlich, Identifying Personal Genomes by Surname Inference, Science No. 339/6117, Januar 2013, 321 ff.

[18] Günter Karjoth, Sind anonymisierte Daten anonym genug?, Digma 2008, 18 ff.

[19] Joachim Dorschel/Philipp Nauerth, Big Data und Datenschutz – Ein Überblick über die rechtlichen und technischen Herausforderungen, Wirtschaftsinformatik & Management, 2013, 34.

dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[20] Dies bedeutet in der Praxis z.B., dass Social-Media Websites ihre Nutzer darüber aufklären müssen, dass sich die gesammelten personenbezogenen Daten durch Big-Data-Technologien in Nutzerprofile wandeln und zur Verhaltensvorhersage verwenden lassen. Ein solcher Hinweis kann an sich im Rahmen von AGB erfolgen, jedoch ist fraglich, ob ein blosser Hinweis einer strengen AGB Kontrolle standhalten würde, weil eine derartige Nutzungsklausel wohl im Allgemeinen vom Nutzer nicht erwartet wird. Es sollte daher ein besonderer Hinweis erfolgen.

Weiterhin ist aufgrund der Pseudonymisierung der Daten auch in der Schweiz fraglich, ob diese sich unter Artikel 4 DSG subsumieren lassen und demzufolge das DSG Anwendung findet.[21] Personendaten sind Daten, welche sich auf eine bestimmbare Person beziehen. Hierbei ist eine Abwägung zu treffen, ob die Pseudonymisierung der Daten zu einem Verlust der Bestimmbarkeit geführt hat oder nicht.[22] Dabei ist wichtig, ob die Daten Teil einer Datensammlung sind, die eine Identifizierbarkeit durch entsprechende Schritte wieder ermöglichen würde oder sie als einzelne Datensätze gespeichert werden, welche ohne Zuhilfenahme einer dritten Datenbank keinen Personenbezug aufweisen. Der Grad der Unkenntlichmachung sowie der Speicherort des «Entschlüsselungsmechanismus» sind daher entscheidend für eine Zuordnung. Im Gegensatz dazu sind anonymisierte Daten keine Personendaten, weil der Personenbezug generell nicht mehr hergestellt werden kann. Für Big Data Analystics sind jedoch komplett anonymisierte Daten nur von begrenztem Interesse, da mit ihnen nur generelle Aussagen getroffen werden können.

Die Gefahr für private Nutzer eines Dienstes liegt in dem oftmals fehlenden Bewusstsein, dass trotz Anonymisierung der Daten diese zur Erstellung von Gruppenprofilen verwendet werden können. Solche Profile fallen aufgrund ihrer Klassifizierung jedoch nicht unter die Europäische Datenschutz-Richtlinie[23] und erhalten keinen besonderen Schutz.[24] Sie erlauben den Unternehmen z.B. im Onlinehandel, Kundengruppen mit ähnlichen Interessen zu identifizieren um diesen

---

20 Art. 4 Abs. 3 DSG (SR 235.1)

21 URS BELSER, in: MAURER-LAMBROU/VOGT (Hrsg.), Datenschutzgesetz, 2. Aufl. Basel 2006, Art. 11 N 7 ff.

22 PAUL OHM, Broken Promise of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review (2010), 1742 f. OHM führt an, dass alle Daten gemäss der Datenschutzgesetzgebung wie personenbezogene Daten behandelt werden sollten.

23 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Erwägung Nr. 26.

24 OMER TENE/JULES POLONETSKY, Big Data for all: Privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property Vol. 5, No. 5, 256–259.

bei einer entsprechenden Suche im Onlineshop Waren anzuzeigen, welche andere Mitglieder der Gruppe gekauft haben. Ein weiterer Anwendungsfall solcher Gruppendaten im Kontext von Big Data ist die Analyse des Stromverbrauchs innerhalb eines Stadtgebiets. In Los Angeles wurde der Stromverbrauch aller Stadtbezirke gemessen und anhand einer Karte in Verbrauchszonen eingeteilt. Dies ermöglicht in Verbindung mit weiteren Informationen (z.B. Einkommensniveau) Rückschlüsse auf das Verhalten der Bewohner wie auch den Zustand der Gebäude. Parallel kann Big Data Analytics zur Überwachung der Einhaltung von Energieeffizienzstandards genutzt werden.[25]

Der Kunde kann jedoch die Bearbeitung der Daten durch vertragliche Nutzungsbeschränkungen steuern. Notwendig wäre dafür indessen der Abschluss eines individuellen Vertrages, der unter Verzicht auf die Verwendung von AGB konkret ausgehandelte Anordnungen zur Art der Datennutzung enthält. Eine solche Vorgehensweise kompliziert nicht nur die Vertragsverhandlungen, sondern entspricht regelmässig auch nicht einem Bedürfnis der Kunden, die sich nicht mit Datenschutzüberlegungen auseinandersetzen wollen. Vielmehr würden individuelle «Vertragsverhandlungen» zum Verlust des eigentlichen Nutzens der Big-Data-Sammlungen führen, weil diese nur mit äusserst hohem Aufwand betrieben werden könnten. Ohne standardisierte Verfahren lässt sich somit den technologischen Gegebenheiten nicht Rechnung tragen.

Findet eine Auswertung von personenbezogenen Social Media Daten statt, hat der Nutzer des Service oftmals seine Einwilligung zu einer solchen Datenverarbeitung bereits durch Einwilligung zu den AGB gegeben. Im Gegenzug kann der Nutzer den Service der Website in Anspruch nehmen. Dieses Vorgehen der Diensteanbieter ist heute weit verbreitet. Selbst einfache «Click-Wrap-Agreements» enthalten Klauseln, welche nicht nur Big-Data-Analysen erlauben, sondern auch eine Haftung, die sich in deren Zusammenhang ergeben, ausschliessen.

Im Einzelnen liegt die Entscheidung, welche Daten als Gegenleistung für einen Service herausgegeben werden und welcher Wert mit diesen Daten verknüpft wird, beim Nutzer selbst. Die Daten werden zwar kostenfrei herausgegeben, jedoch ist aufgrund der Analysemethoden durch Big Data ein realer Wert mit ihnen verknüpft.[26] Es ist somit wichtig, dass die Leistung und deren Preis vertraglich klar umschrieben sind, um spätere Probleme z.B. steuerrechtlicher Natur zu begrenzen. Dies zeigt, dass die Privatsphäre, welche vormals durch den Staat geschützt

---

[25] MARTIN LAMONICA, Los Angeles Maps Electricity Use at the Block Level, MIT Technology Review (http://www.technologyreview.com/view/512991/los-angeles-maps-electricity-use-at-the-block-level/)

[26] THE BOSTON CONSULTING GROUP, The Digital Manifesto, How Companies And Countries Can Win In The Digital Economy, Januar 2012.

wurde, heute zum grossen Teil nur auf Basis der Zahlungsbereitschaft der Kunden erhalten werden kann.[27]

Es bleibt abzuwarten ob die Nutzer von Onlinediensten bereit sind, für ihre Privatsphäre zu bezahlen. Vornehmlich wird dabei die Zurverfügungstellung von einfachen Bezahl- und Überwachungssystemen eine grosse Rolle spielen.[28]

2. Regelung von Eigentums- und Lizenzrechten

Insbesondere bei wertvollen Daten ist vertraglich zu regeln, wer die Eigentumsrechte an den Daten hält und ob sich an den Eigentumsrechten mit den Datenbearbeitungen, d.h. der Schaffung eines neuen Datensatzes, etwas ändert. Die Frage stellt sich ebenfalls für die Daten, welche durch eine Big-Data-Analyse gewonnen werden und die den eigentlichen Wert darstellen. Der Gebrauch der Daten und das Recht auf Veränderung der Daten sind im Kontext einer Lizenzeinräumung an den Dienstleistungserbringer zu konkretisieren. Eine solche Lizenzeinräumung ist in der Regel kostenfrei, weil das Dienstleistungsunternehmen, das die Lizenz eingeräumt erhält, für den Kunden durch die Big Data Analytics einen Mehrwert zu erreichen versucht.

Generell sind Werke individuellen Charakters, d.h. persönliche geistige Schöpfungen der Literatur, Wissenschaft und Kunst, die eine «minimale» Schöpfungshöhe erreichen, urheberrechtlich geschützt (Art. 2 URG).[29] Im Kontext von Big Data geht es bei der Beurteilung der Zulässigkeit von Datenanalysen und Datenauswertungen somit vornehmlich um die Frage, ob die verfügbaren Daten frei verwertbar sind oder nicht.[30]

Im Durchschnitt besitzt jedes Unternehmen rund 125 TB an Daten, die potenziell für Big Data Analytics verwendet werden können.[31] Das schnelle Wachstum dieser Datenbestände wird insbesondere durch sehr günstige Cloud-Anbieter wie Amazon und Google in Verbindung mit kostenfreier Open-Source Software wie

---

27 DENISE JEITZINER, Die meisten gehen davon aus, dass der Staat sie schützt, Tagesanzeiger online 5.3.2013. (http://www.tagesanzeiger.ch/kultur/diverses/Die-meisten-gehen-davon-aus-dass-der-Staat-sie-schuetzt/story/29790039?track)

28 TOM SIMONITE, If Facebook can profit from your data, why can't you?, MIT Technology Review, 30 July 2013, (http://www.technologyreview.com/news/517356/if-facebook-can-profit-from-your-data-why-cant-you/)

29 RETO M. HILTY, Urheberrecht, Bern 2011, § 6 N 83 ff.

30 Für eine detaillierte Besprechung der urheberrechtlichen Fragestellungen vgl. ROLF H. WEBER, Big Data: Rechtliche Perspektiven, in diesem Band, 17–29.

31 JUDE UMEH, Big Data, Privacy And Intellectual Property. (http://www.Capgemini.Com/Blog/Capping-It-Off/2013/09/Big-Data-Privacy-And-Intellectual-Property).

z.B. Hadoop begünstigt. Unter diesen Daten vermögen sich unterschiedlichste urheberrechtlich geschützte Daten zu befinden. So ist es denkbar, dass das Unternehmen selbst Eigentümer von Rechten ist, eine dritte Partei das Urheberrecht besitzt oder es sich um open source Daten handelt, welche keinem besonderen Schutz unterliegen. Die Menge dieser gesammelten Daten wächst exponentiell und stellt damit bestehende IT-Systeme vor grosse Herausforderungen. Unter anderem muss sichergestellt werden, dass ein Unternehmen in der Lage ist, diesen Datenbestand zu verstehen, um erkennen zu können, welche Daten möglicherweise urheberrechtlich geschützt sind bzw. besonderer Sicherheitsmassnahmen wegen ihrer Sensibilität bedürfen.

Aufgrund der sich ständig verändernden Strukturierung von Datenbeständen und deren Nutzung sind die Algorithmen zur Datenauswertung kontinuierlich anzupassen. Der vertragliche Rahmen zwischen einem Big-Data-Provider und dem Unternehmen, welches die Daten zur Bewirtschaftung zur Verfügung stellt, muss daher in der Lage sein, die hierfür notwendige Flexibilität zu gewährleisten. Diese Veränderlichkeit erschwert wiederum die Durchsetzung von urheberrechtlich geschützten Rechten an Algorithmen und Daten, weil sich diese in einer ständigen Anpassung und damit im Fluss befinden.

Sonderregelungen sind zu treffen, wenn Geschäftsgeheimnisse eine besondere Rolle spielen. Sollte der Eigentümer der Daten an gewissen Geschäftsgeheimnissen ein Patent- oder ein Urheberrecht erworben haben, finden die allgemeinen immaterialgüterrechtlichen Regelungen Anwendung. Sonst ist zu prüfen, ob spezifische vertragliche Schutznahmen einzuführen sind.

Auch mit Blick auf Geschäftsgeheimnisse stellen sich Fragen der Datensicherheit; um Risiken zu minimieren, sind gegebenenfalls die Verbreitung und Bearbeitung entsprechender geschützter Daten zu verschlüsseln. Zurzeit wird verstärkt an neuen Technologien, welche eine Nutzung d.h. Bearbeitung der verschlüsselten Daten ermöglichen soll, geforscht.[32]

3. Vorgaben zur Qualitätssicherung

Von grosser Bedeutung ist weiter der Bereich der Umschreibung der Qualität von Dienstleistungen; gerade angesichts der Sensitivität von Big-Data-Analysen sind neben den allgemeinen Qualitätsanforderungen («state of the art») auch kundenspezifische Konkretisierungen vorzunehmen. Die Einzelheiten hängen von den konkreten Gegebenheiten ab.

[32] Führend in diesem Bereich ist u.a. Prof. Alex Pentland vom Massachusetts Institute of Technology (http://www.Media.Mit.Edu/People/Sandy).

Im Kontext der Qualitätsanforderungen ist weiter das Abnahmeverfahren bzw. das Testverfahren mit Blick auf erbrachte Dienstleistungen zu regeln. Eingeschlossen sein sollten zudem die Kontrollrechte des Kunden. Änderungen mit Blick auf die Dienstleistungsqualität bedürfen jedenfalls der Zustimmung des Kunden.

Aufgrund der Fülle an verarbeiteten Daten müssen die Kundenwünsche genau spezifiziert werden, um sicherzustellen, dass die durch eine Big-Data-Analyse gewonnen Daten auch das gewünschte Ergebnis tatsächlich abbilden. Dazu ist von Seiten des Big-Data-Providers ein detaillierter Plan zu entwerfen und die zu verwendenden Daten sind präzise zu beschreiben. Des Weiteren lassen sich vertragliche Regelungen hinsichtlich der Haftung bei Verstoss gegen das Datenschutzgesetz treffen, um den Big-Data-Provider vor Kosten zu schützen, welche durch die illegale Sammlung von Daten durch den Kunden unter Umständen entstehen könnten.[33] Insbesondere ist in solchen Vereinbarungen auch auf die nachfolgende Haftung durch eine unsachgemässe Nutzung und eventuelle Publikation einzugehen.

Ein Big-Data-Nutzer sollte fortlaufend die ausgeführten Berechnungen hinterfragen, weil sich zum Teil Korrelationen ergeben können, die willkürlich entstehen und daher zu falschen Schlussfolgerungen führen. Dadurch entsteht ein Geschäftsrisiko, dem durch regelmässige Kontrollen entgegenzuwirken ist. Insbesondere können schnell grosse Verluste entstehen, wenn auf Basis der gewonnenen Daten zielgerichtete Werbung durchgeführt wird. Der Effekt der Werbung verpufft unter diesen Umständen ohne den gewünschten Erfolg.[34]

4. Compliance

Angesichts der Sensitivität vieler Big-Data-Analysen kommt der vertraglichen Vereinbarung von Compliance-Massnahmen grosse Bedeutung zu. Denkbar ist, vertraglich vorzusehen, dass der Kunde gewisse Vorgänge beim Dienstleistungserbringer auditieren darf (z.B. Art und System der Aufbewahrung). Weiter muss die Möglichkeit bestehen, eine Compliance mit Blick auf die Einhaltung der vereinbarten Dienstleistungsstandards vorzunehmen. Alternativ müssen unabhängige Zertifizierungen geschaffen werden, um die Vergleichbarkeit der angebotenen Dienste zu ermöglichen.

---

[33] Vgl. RALF BLAHA/ROLAND MARKO/ANDREAS ZELLHOFER/HELMUT LIEBEL, Rechtsfragen des Cloud Computing, Medien und Recht Verlag, Wien 2011, 44.

[34] PHILIPP LÖPFE, Wir sind viel vorhersehbarer, als wir glauben, Tagesanzeiger online 7.1.2014, (http://www.tagesanzeiger.ch/wissen/Wir-sind-viel-vorhersehbarer-als-wir-glauben/story/22290710?track).

Big-Data-Mechanismen werden zunehmend komplexer, was eine Überwachung und Kontrolle zukünftig für einen individuellen Datenlieferanten verunmöglicht. So entwickelt Google derzeit eine künstliche Intelligenz, welche auf Basis der immensen Big-Data-Speicher dem Nutzer der Google-Suchmaschine bereits Ergebnisse vorschlägt, welche auf diesen zugeschnitten sind, aber noch nicht vom Nutzer durch eine Suche angefordert wurden.[35] Mit dieser Technologie soll eine möglichst exakte Einschätzung des zukünftigen Verhaltens eines jeden Nutzers ermöglicht werden.[36]

Ein besonderer Bereich betrifft die Sicherstellung der «betrieblichen» Kontinuität der Geschäftsaktivitäten. Probleme verursachen können nicht nur grosse technische «Abstürze», sondern auch die fehlende finanzielle Stabilität des Dienstleistungserbringers. Due-Diligence-Massnahmen mit Blick auf die technische Robustheit des Gesamtsystems als auch hinsichtlich der finanziellen Leistungsfähigkeit des Dienstleistungserbringers sind deshalb angebracht. Die Grenze vertraglicher Absprachen dürfte bei den Geschäftsgeheimnissen des Dienstleistungserbringers liegen.

Besonders komplex ist die vertragliche Vereinbarung von Compliance-Massnahmen mit Bezug auf Dienstleistungen, die von Unterbeauftragten erbracht werden. Im Kontext von Big-Data-Berechnungen werden oftmals eine Vielzahl von Unterbeauftragen verwendet. So kann z.B. die Berechnung in der Cloud stattfinden, was es dem Anbieter ermöglicht, einen IaaS-Cloud-Provider zu wählen, welcher die benötigte Hardwarekapazität zur Verfügung stellt, und einen SaaS-Provider, der die entsprechend benötigte Software bereitstellt.[37]

Indessen muss gewährleistet sein, dass keine Rechte von Drittparteien verletzt werden. Dies kann vertraglich durch die Einräumung eines Rechts des Datensubjekts zur Vornahme von Kontrollen, wie auch einer angepassten Haftungsklausel geschehen. Durch diese Massnahmen erhält die unbeteiligte Drittpartei, deren persönliche Daten durch einen Unterbeauftragten genutzt werden, sofort durchsetzbare Rechte gegenüber diesem. Jedoch verbleiben die bekannten Probleme in Fällen, in denen die Daten in ein anderes Land transferiert werden und somit die Vollstreckung der vertraglich zugesicherten Forderungen sich als schwierig gestaltet.

---

35 Interview by KEITH KLEINER with RAY KURZWEIL, Director of Engineering, Google, in: Moffett Field, Cal. (Jan. 4, 2013). (http://www.youtube.com/watch?v=yabuffpqy9w).

36 IAN KERR/JESSICA EARLE, Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, 66 Stan. L. Rev. Online 65, 67.

37 Vgl. SIMON BRADSHAW/CHRISTOPHER MILLARD/IAN WALDEN, Standard Contracts for Cloud Services, in: CHRISTOPHER MILLARD (ed.), Cloud Computing Law, Oxford 2013, Chapter 3, 39 ff.

Im Einzelfall sind die anwendbaren Vorschriften jedes Staates, in welchem der Big-Data-Provider tätig ist, genau zu prüfen. So hat z.B. Kalifornien in 2013 seine Datenschutzgesetzgebung angepasst um den Kunden, deren Daten von verschiedensten Unternehmen genutzt werden, grössere Rechte einzuräumen. Sie müssen nun ihren Kunden nach Aufforderung innerhalb von 30 Tagen eine Kopie der gespeicherten Daten herauszugeben. Ebenfalls müssen sie darüber informieren an welche Drittparteien Daten innerhalb der letzten 12 Monate weitergegeben wurden. Das Unternehmen kann dabei einen von verschiedenen im Gesetz vorgegebenen Kommunikationswegen wählen. Ein Verstoss gegen diese Bestimmung wird automatisch als Schädigung des Kunden gewertet was eine Schadenshaftung zur Folge hat. Die Anwendung des Gesetzes erstreckt sich jedoch nur auf die Einwohner von Kalifornien.[38]

Zu beachten sind ebenfalls die Risiken, welche sich durch die Insolvenz des Anbieters ergeben können. Dabei bieten vertragliche Regelungen nicht in allen Situationen eine Lösung, weil meist das jeweils einschlägige nationale Konkursrecht spezifische Regelungen vorsieht. Somit ist das vorherrschende Recht bei der Wahl des Anbieters an dessen Serverstandort zu beachten. Zumal internationale Datentransfers heute üblich sind, ist sicherzustellen, dass vertragliche Vereinbarungen getroffen werden, die den Umfang und die Destination solcher Übertragungen gemäss dem notwendigen Datenschutz und Sicherheitsbedürfnis des Kunden einschränken.

IV. Haftungsbeschränkung und Haftungsfreizeichnung

Im Big-Data-Geschäft ist zwischen dem Verhältnis eines Diensteanbieters zum Privatkunden, welcher persönliche Informationen zur Verfügung stellt, und der Beziehung zwischen dem Diensteanbieter und einen Big-Data-Serviceanbieter zu unterscheiden. Der Diensteanbieter kann bei entsprechender Grösse und Infrastruktur eigene Datensammlungen erstellen und Berechnungen durchführen oder diese an einen Big-Data-Anbieter auslagern.

Grosse Anbieter von Big-Data-Analyseleistungen versuchen regelmässig, in vorformulierten Verträgen das eigene Risiko durch Haftungsbeschränkungen und Haftungsfreizeichnungen soweit als möglich zu limitieren. Dabei ist deren Durchsetzungsvermögen jedoch bei einem finanzstarken Geschäftspartner Grenzen ge-

[38] Section 1798.83 Civil Code California (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84)

setzt. Ist der Kunde jedoch umsatzmässig unbedeutend, hat er nur geringe Möglichkeiten, die vorgelegten Verträge anzupassen. Oftmals sind es jedoch auch grössere Unternehmen, die Big-Data-Leistungen in Anspruch nehmen. Diese sind weniger bereit, das gesamte Geschäftsrisiko auf sich zu nehmen, und erwarten daher vermehrte Zugeständnisse der Big-Data-Provider. Diese wiederum reduzieren ihr Risiko, indem sie entsprechende Versicherungen abschliessen, welche den potenziellen Verlust begrenzen.

Unter anderem sind der Verlust der Daten oder die unerlaubte Herausgabe von Daten oder Berechnungsergebnissen für einzelne Kundenkreise besonders wichtig. Die Handlung (selbst fahrlässiger Art) stellt schon einen schweren Verstoss gegen den Datenschutz sowie die vertraglichen Vereinbarungen mit dem Kunden dar. Jedoch ist in einzelnen Fällen die Vernichtung der Daten viel gravierender, z.B. wenn diese für ein Gerichtsverfahren benötigt werden.[39]

Insbesondere die Nutzung der Big-Data-Technologie im vornehmlich angelsächsischen eDiscovery-Prozess stellt hohe Anforderungen an die Datensicherheit sowie die Geheimhaltung. In einem solchen Szenario wäre der Schaden, welcher dem Kunden durch eine unerlaubte Preisgabe an Informationen entstehen könnte, sehr gross. Unter Umständen sind sogar strafrechtliche Konsequenzen für die verantwortlichen Manager denkbar, insbesondere in Situationen, in denen Informationen, welche für ein Gerichtsverfahren notwendig sind, zerstört wurden. Als wirksame Abschreckung sind diese zu begrüssen. Für die Nutzer von Big-Data-Diensten und deren Klienten ist es ebenso wichtig, dass der Big-Data-Anbieter entsprechende Versicherungen abschliesst und in der Lage ist, für einen eventuell entstehenden zivilrechtlichen Schaden aufzukommen. Weiterhin müssen in Abhängigkeit von den vorhandenen Daten verstärkte Sicherheitsmassnahmen vertraglich vereinbart werden.

V. Ausblick

Angesichts der Datenmenge und Komplexität der Datenstrukturen in Big Data sind Systeme wie z.B. Zertifikate zu entwickeln, die es dem einzelnen Nutzer erlauben, seinen gewünschten Datenschutz selbst anhand vorgegebener Kriterien zu bestimmen. Mit einem solchen individuellen und doch einheitlichen Vorgehen lässt sich dem Wunsch der Big-Data-Provider nach einer zuverlässigen und rechtssicheren Lösung Rechnung tragen. Der Datenschutz und die Übersichtlichkeit für den einzelnen Nutzer von Onlinediensten bleibt dabei ebenfalls gewahrt,

[39] Vgl. Alberto G. Araiza, Electronic Discovery in the Cloud, Duke Law & Technology Review 10 (2011), 1–19.

wodurch sich dieser sicher sein kann, dass seine Daten, ungeachtet der Nutzung welches Dienstes, denselben von ihm vorgegebenen Schutz erfährt. Hierzu bedarf es jedoch eines einheitlichen Vorgehens der EU und der Schweiz, um ein solches System bindend für alle Anbieter vorzuschreiben, welche auf dem EU/Schweizer Markt tätig sind.

Zudem verbleiben die bestehenden Problemstellungen des Datentransfers ausserhalb des EU/Schweizer Raums. Dort kann der Datenschutz nicht gewährleistet werden, weil bis heute, mit Ausnahme des Sale Herbor Agreement (USA), hierzu keine internationalen Abkommen existieren. Vertragliche Vereinbarungen sind in dieser Hinsicht meist inadäquat, weil sie keinen Einfluss auf die Zugriffsrechte der Drittstaatenbehörden nehmen können.[40]

Im «Business-to-Customer»-Geschäft sollten die Diensteanbieter, welche die erworbenen personenbezogenen Daten in einer Big-Data-Lösung gewinnbringend verarbeiten möchten, in übersichtlicher Form vertraglich darlegen, für welchen Zweck die Daten eingesetzt werden können. Den Kunden ist zudem eine Möglichkeit einzuräumen, seine Daten auf Wunsch löschen zu lassen.

Im Fall der Nutzung eines Big-Data-Drittanbieters durch den eigentlichen Diensteanbieter muss dieser sicherstellen, dass die durch ihn mit dem Kunden eingegangenen Verpflichtungen auch gegenüber dem Unterbeauftragten durchsetzbar sind. Insoweit bedarf es klarer gesetzlicher Rahmenbedingungen, um sowohl für den Nutzer als auch den Diensteanbieter Rechtssicherheit zu schaffen.

Die Möglichkeiten, welche sich durch Big Data ergeben, scheinen unbeschränkt. So ist es in den USA bereits Realität, dass mit Hilfe solcher grossen Datenbestände Gruppierungen zielgerichtet von den Geheimdiensten identifiziert werden können. Dieser Personenkreis wird dann aufgrund einer Computerberechnung pauschal verstärkter Überwachung ausgesetzt. Ebenso kann Big Data Personenkreise identifizieren, welche für die Unternehmen nicht gewinnbringend sind. Diese werden hernach allmählich an den Rand der Gesellschaft gedrängt.[41] Es scheint daher zumindest als angebracht, die Kunden, die meist nichtsahnend ihre persönlichen Informationen preisgeben, adäquat über die Möglichkeiten, die zur Auswertung ihrer Daten bestehen, zu informieren. Hierzu sind zukünftig einfache und übersichtliche Systeme erforderlich. Der Gesetzgeber ist daher gefordert, die entsprechenden Rahmenbedingungen im Datenschutz und im Vertragsrecht zu schaffen, um den zum Grossteil gegensätzlichen Interessen der Big-Data-Anbieter und Privatpersonen Rechnung zu tragen.[42]

---

[40] WEBER/STAIGER (Fn. 15), Rz. 45 ff.
[41] Plessy v. Ferguson, 163 U.S. 537, 559 (1896) (Harlan, J. dissenting).
[42] KERR/EARLE, (Fn. 33), 69.

Ungeachtet des enormen Potenzials von Big Data ist der Schutz jeder dieser Datensätze und der dahinter stehenden Personen zu gewährleisten. Das Gegenteil dieser Idealsituation wurde 2008 eindrücklich durch Google demonstriert. Unter anderem hat Google Wissenschaftlern erlaubt, die gesammelten Daten der Suchmaschinennutzer hinsichtlich gewisser Schlüsselwörter zu filtern, mit dem Ergebnis, dass Grippeausbrüche in einzelnen Regionen identifiziert werden konnten. All dies geschah jedoch ohne Wissen oder Zustimmung der einzelnen Nutzer.[43]

VI. Anhang

Vertragscheckliste für Big-Data-Anwendungen auf Basis einer Cloud-Plattform[44]

1. Benennung der Vertragsparteien

1.1 Big-Data-Anwender und einzelner Cloud-Provider (single vendor model)

1.2 Big-Data-Anwender und mehrere Cloud-Provider (multi vendor model)
- Rechtliche und technische Rahmenbedingungen festzulegen durch den Big-Data-Anwender
- Generalunternehmer-Modell (vendor management)

2. Festsetzung des Vertragsgegenstands

3. Benennung der Hauptpflichten des Providers

3.1 Art des Cloud Service
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

3.2 Welche Partei stellt die Datenanbindung zur Verfügung?

3.3 Wo findet die Datenspeicherung und Bearbeitung statt (Länderwahl?)

4. Weitere Leistungen des Providers

4.1 Support

4.2 Wartung

---

[43] Google.Org, Tracking Flu Trends, The Official Google.Org Blog. Http://Blog.Google.Org/2008/11/Tracking-Flu-Trends.Html (Explaining The Methodology Employed By Google To Track The Spread Of Influenza).

[44] Vgl. auch RALF BLAHA/ROLAND MARKO/ANDREAS ZELLHOFER/HELMUT LIEBEL (Fn. 33), 61–64.

4.3 Helpdesk

4.4 Schulungen

4.5 Backups (Intervall/Zugriff/Schutz)

4.6 Datenpflege (Art und Umfang)

5. Wie wird der Service zur Verfügung gestellt (Deployment-Modell)?

5.1 Private Cloud

5.2 Public Cloud

5.3 Hybride Formen

6. Ist der Einsatz von Subunternehmen erlaubt? Bedingungen?

7. Service Level Vereinbarungen

7.1 Verfügbarkeit des Cloud Service (Prozentsatz über welchen Zeitraum?/ max. zulässige Ausfallzeit)

7.2 Reaktions- und Fehlerbehebungszeiten

7.3 Aufzeichnung, Überwachung und Meldung von Problemen

7.4 Sanktionen bei Vertragsbruch bzw. Ausfällen, Kündigungsrecht

8. Mitwirkungspflichten des Big-Data-Anwenders

8.1 Erfüllung bestimmter Systemvoraussetzungen?

8.2 Einhaltung von Regeln zur Nutzung und Bedienung des Systems

9. Nutzungsrecht

9.1 Nutzungsrecht für erforderliche Software

9.2 Ggf. eine «catch all» Klausel, welche alle für die Big-Data-Cloud-Berechnung erforderlichen Nutzungsrechte einräumt

9.3 Nutzungsrechte von Seiten der Datenlieferanten der Big-Data-Datensätze

9.4 Bestimmung der Eigentums und Nutzungsrechte an den erzeugten Datensätzen

10. Festsetzung des Entgelts

10.1 Pauschales Entgelt/Pro Einheit?

10.2 Zahlungsbedingungen?

10.3 Eventuelle Vergünstigungen bei Erreichung eines Nutzungslevels

11. Change Management

11.1 Leistungsänderungsrechte sind genau zu spezifizieren und von der Skalierbarkeit des Service abzugrenzen

11.2 Rahmenbedingungen der Anpassung (Zulässigkeit, Zeitpunkt)

12. Gewährleistung und Haftung

12.1 Basierend auf der Leistungsbeschreibung Feststellung möglichst abschliessende Sanktionen für Nicht-/Schlechtleistung

12.2 Klare Spezifizierung von Haftungsausschlüssen und Haftungsbeschränkungen

12.3 Versicherungen des Cloud-Providers sowie des Big-Data-Anwenders

12.4 Haftung des Big-Data-Anwenders wenn Handlungen Auswirkungen auf andere Cloud-Nutzer zeitigen (selbe Hardware durch Virtualisierung)

13. Geheimhaltung und Datenschutz

13.1 Verpflichtung zur Vertraulichkeit

13.2 Verpflichtung zur Einhaltung des Datenschutzes
- Kontrollrechte
- Einbezug von Subdienstleistern
- Meldung von Datenschutzverstössen

13.3 Regelung des grenzüberschreitenden Datenverkehrs

14. Eskalation, Notfall- und Exit-Management

14.1 Streitbeilegungsverfahren

14.2 Notfallmanagement bei betriebskritischen Störungen

14.3 Exit Management
- Datenherausgabe (Format)
- Unterstützung durch Cloud-Provider?

15. Vertragsdauer und Kündigungsrechte

16. Schlussbestimmungen

16.1 Verjährung

16.2 Rechtswahl

16.3 Gerichtsstand

16.4 Formerfordernisse

16.5 Zession-/Aufrechnungsverbot

16.6 Salvatorische Klausel

ZIK

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Big Data und Datenschutz – Gegenseitige Herausforderungen

Schulthess § 2014

59

Inhaltsverzeichnis